

Information for Parliamentarians

Shared Services Canada

Network Modernization and Procurement

02-24-2021 | Version 3.0



Shared Services
Canada

Services partagés
Canada

Canada

Network Modernization: Quick Facts

40+

The number of network infrastructures inherited by Shared Services Canada from government organizations upon its creation.

50

The number of aging network infrastructures.

4,000

The number of network sites in Canada and across the world that require Shared Services Canada's attention.

300,000

The number of Secure Remote Access connections for public servants to work remotely and securely.

Network and Procurement: At a Glance

- Shared Services Canada (SSC) was created in 2011 to provide integrated and reliable digital solutions to public servants for the delivery of government services to Canadians.
- SSC inherited the different and varied network infrastructure with a large footprint from government organizations. SSC was mandated to consolidate and standardize the Government of Canada information technology (IT) infrastructure, before any modernization work could start.
- SSC has a very ambitious digital agenda. While a lot of work has been done over the past nine years, there remains a significant backlog of aging network infrastructure.
- It is critical that products are interoperable to work with other components of the existing infrastructure. When SSC procures new equipment, the bidder must propose equipment that is compatible, interoperable and/or interchangeable with existing equipment.
- SSC's efforts to modernize and strengthen the foundation of the Government of Canada's digital infrastructure is critical to the continuous and secure delivery of essential services, and to an improved experience of Canadians.
- SSC is focused on building a more secure, stable and agile environment for the Government of Canada's (GC) digital operations, and SSC continues to consolidate, standardize and modernize networks across the federal departments. The repair and replacement of existing equipment will continue in tandem with SSC's modernization plans for the foreseeable future.
- When COVID-19 hit, the use of an integrated and consolidated IT infrastructure is what allowed SSC to enable digital services and virtual work for employees so quickly.
- SSC continually improves the way it delivers its business: a [Network Modernization Way Forward](#) discussion paper was developed to identify future requirements, and the Department is engaging industry on its network and procurement needs to seek input, leverage innovation and build an adapted procurement vehicle.
- SSC has increased diversification in its procurement of network components and made great strides to engage small and medium enterprises (SME) and to build greening in its requirements. To reduce its reliance on any one vendor, SSC will continue to maximize its use of competitive processes to open up the competition to a multitude of vendors, acquire equivalent equipment and directed original-equipment-manufacturer (OEM) purchases on a case by case basis.
- SSC has robust procurement governance and practices including reliance on external expert reviews and audit to inform continuous improvement.



A Vision for the Future – The Strategy Moving Forward

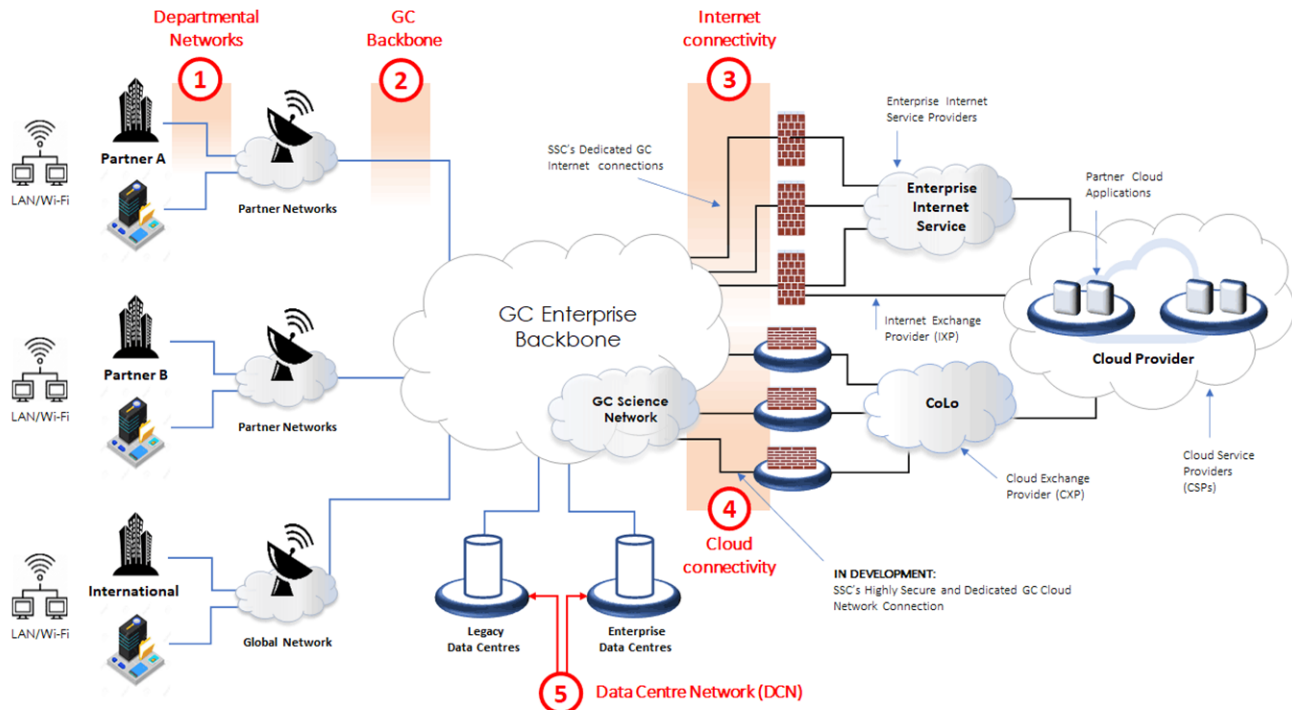
Network security is more important than ever as Canadians access more programs and services online. Protecting the government's IT infrastructure from vulnerabilities and responding to cyber security related attacks is critical to the safety and security of Canadians' data and of services provided by the Government of Canada.

To effectively deliver services to Canadians, the federal government is investing resources to develop a dependable, fast, secure and reliable network to deliver programs and services to Canadian businesses and citizens.

The recent COVID-19 pandemic resulted in a dramatic shift in the federal government's network landscape with the vast majority of public servants suddenly being forced to work from home. It is expected that public servants will continue to work from home or adopt a hybrid office/home work environment in the future. These factors, coupled with technical innovations such as software-defined infrastructure (SDI), where critical IT functions within a network and data centre are fully automated and programmable, and improved wireless technology, have caused SSC to reassess how it delivers and secures network services. A modernized approach, leveraging software-defined infrastructure and artificial intelligence (AI), provides both improved manageability and performance to enable the Government of Canada's "cloud-first" strategy. Now is the time to ensure our strategy is aligned with current best practices and is adaptable to future requirements for its network and security services.

To this end, SSC is engaged in a collaborative process to update the GC's Enterprise Network and Security Strategy, to be transparent about our future directions and ensure that we achieve a future state that meets Government's needs. Last month, we published the "[Network Modernization Way Forward](#)" to solicit feedback from our various partners and stakeholders on this future state. The draft GC Enterprise Network and Security Strategy will also be made available shortly for comment. SSC wants to hear from industry, as well as from partner departments and agencies and other stakeholders, to ensure that we develop an updated Strategy, and a strong and secure network in partnership. Transparency and open dialogue with industry and partners is essential to this process.





Networking and Procurement – Mythbusters

Myth: Shared Services Canada (SSC) is determined to buy only Cisco infrastructure in the future

Fact: SSC is vendor agnostic and committed to openly competing procurement activities. Decisions about which technologies to acquire are determined by the specific requirements of each individual project. The Department uses directed buys for Cisco equipment (or equivalents) only when there is a technical requirement to do so.

SSC is currently designing the future state network solution, and establishing corresponding contracting vehicles to deliver new Enterprise Network Services. As we move forward with network modernization, SSC will move to standards-based generic technologies where possible, which offer compatibility and will continue to seek competitive solutions from industry leaders.

SSC's Network and Security Strategy is aligned with current best practices and is adaptable to future requirements for its network and security services.

The key business drivers for the Network and Security Strategy include:

- Increasing the operational efficiency of the delivery and management of services through standardization and simplification;
- Defining a network platform that allows for seamless end user mobility — anytime/anywhere from GC approved devices;
- Enhancing the overall security posture of Network services;
- Increasing network performance to enable the next generation of network services;
- Improving resiliency of the overall network platform thereby reducing the number of incidents and outages;



- Ensuring that technology is accessible for everyone, irrespective of business-model, size, or exclusive rights portfolio. The move towards open standards will open up competition to a multitude of networking vendors, increasing competition and eliminating the federal government's reliance on any one vendor;
- Automating and simplifying critical IT functions within a network to better monitor and manage networks; and
- Designing enterprise network services with users in mind and with the ability to quickly scaled up or down services based on demand. Key to our modernization efforts will be the move towards open standards, which will open up competition to a multitude of vendors, increasing competition and eliminating the federal government's reliance on any one vendor.

SSC regularly consults with industry to make transparent and validate its strategic direction and ensure it is acquiring and deploying the right technologies and getting the best pricing from vendors to deliver maximum value for Canadians. These consultations take numerous forms and include vendors, industry associations and third-party experts.



Myth: SSC awards sole source contracts to Cisco that could be openly competed.

Fact: Whenever possible, SSC uses competition to get the best value for Canadians. At times it is necessary to issue tenders for brand-name products. For example: when purchasing equipment for an existing network comprised of such products, technical requirements may dictate what products can be installed without compromising stability or security. When a brand name is indicated in the requirements, vendors have the option to bid equivalent products that meet the minimum requirements of the tender.

When established in 2011, Shared Services Canada inherited a large, complex network infrastructure. To maintain existing infrastructure, it is essential to acquire equipment that is compatible with what we already have. This ensures continued services to federal organizations who provide important services to Canadians. We are continuously working to maintain the Government of Canada network and legacy networks until such a time as they can be modernized.

As we move forward with network modernization, we will incorporate more standardized and generic technologies, where possible, that offer more compatibility. We will continue to seek competitive solutions from industry leaders.

SSC awarded a total of 153 Cisco related contracts last fiscal year valued at approximately \$145 million. Contracts were issued to 25 different resellers of Cisco, 22 of which are SMEs. Some of the Cisco technology requirements have been procured via OEM specified procurements, but other requirements have been openly competed with the Cisco technology solution being the winning bid.

(SSC executed 2,855 procurement processes for the Government of Canada in fiscal year 2019–2020. Of these:

- 1,645 were competitive, amounting to a total spend of roughly \$1.13 billion.
- 1,210 were non-competitive, amounting to a total spend of roughly \$170 million.

Myth: There has been plenty of time since SSC's creation to hold competitive Requests for Proposals on networking gear. Much of SSC's infrastructure has been refreshed several times since 2011.

Fact: While some elements of the Government of Canada's infrastructure have been refreshed in the 10 years since SSC was created, this is not true for everything. The current digital landscape resides on a highly complex system of network infrastructure that SSC inherited from departments and agencies (referred to as SSC's partners) when it was created 10 years ago. The operational lifecycle for many networking products can run to 20 or 30 years. This equipment is intended and expected to function as an organization's network backbone for many years. SSC must maintain such equipment, as needed, until the government has maximized its return on investment and/or the equipment in question reaches end-of-life and needs to be replaced.

SSC is building a more secure, stable and agile environment for the Government of Canada's digital operations, and continues to consolidate, standardize and modernize networks across the federal departments. The refresh of existing equipment will continue in tandem with the department's modernization plans for the foreseeable future.



Myth: The requirement that new equipment is “interoperable” with existing purchases is just an excuse to buy more Cisco products.

Fact: The Government of Canada’s current digital landscape resides on a highly complex system of network infrastructure throughout the country. This landscape includes approximately 50 networks spanning more than 4,000 sites in Canada and around the world.

There remains a significant backlog of aging network infrastructure that needs to be refreshed with products that ensure compatibility with existing systems. It is critical that products are interoperable with components of the existing infrastructure to maintain the stability and security of the network. Other benefits include a lower maintenance demand, a lower Total Cost of Ownership and increased organizational efficiency.

Interoperability can mean different things to different people in different circumstances and is of particular concern for healthcare, telecommunications, software, online search military, public safety and government stakeholders. For SSC, interoperability refers to the ability of different systems, devices, applications or products to connect and communicate in a coordinated way. Interoperable components provide seamless data access, data transmission and cross-organizational collaboration regardless of their developer or origin. This is usually enabled by the use of common engineering and software standards between manufacturers. For SSC, a critical requirement for the use of interoperable components is their ability to seamlessly fit into the Government of Canada’s existing IT infrastructure.

Interoperability increases complexity and costs. It is a balanced choice and there is a price. It is similar to replacing parts in a car. Using another manufacturer’s parts in a car is possible but could require customization—both with how the pieces interact with each other and are recognized by the car’s software. This could impact efficiency, increase overall costs, and possibly void the warranty. There are also aftermarket/generic parts designed to work with a specific make of car, but even then the fit may require additional work and cause complications. Imagine this same issue for a network infrastructure made of tens of thousands of components. Interoperability has benefits but adds exponentially more complexity and cost.

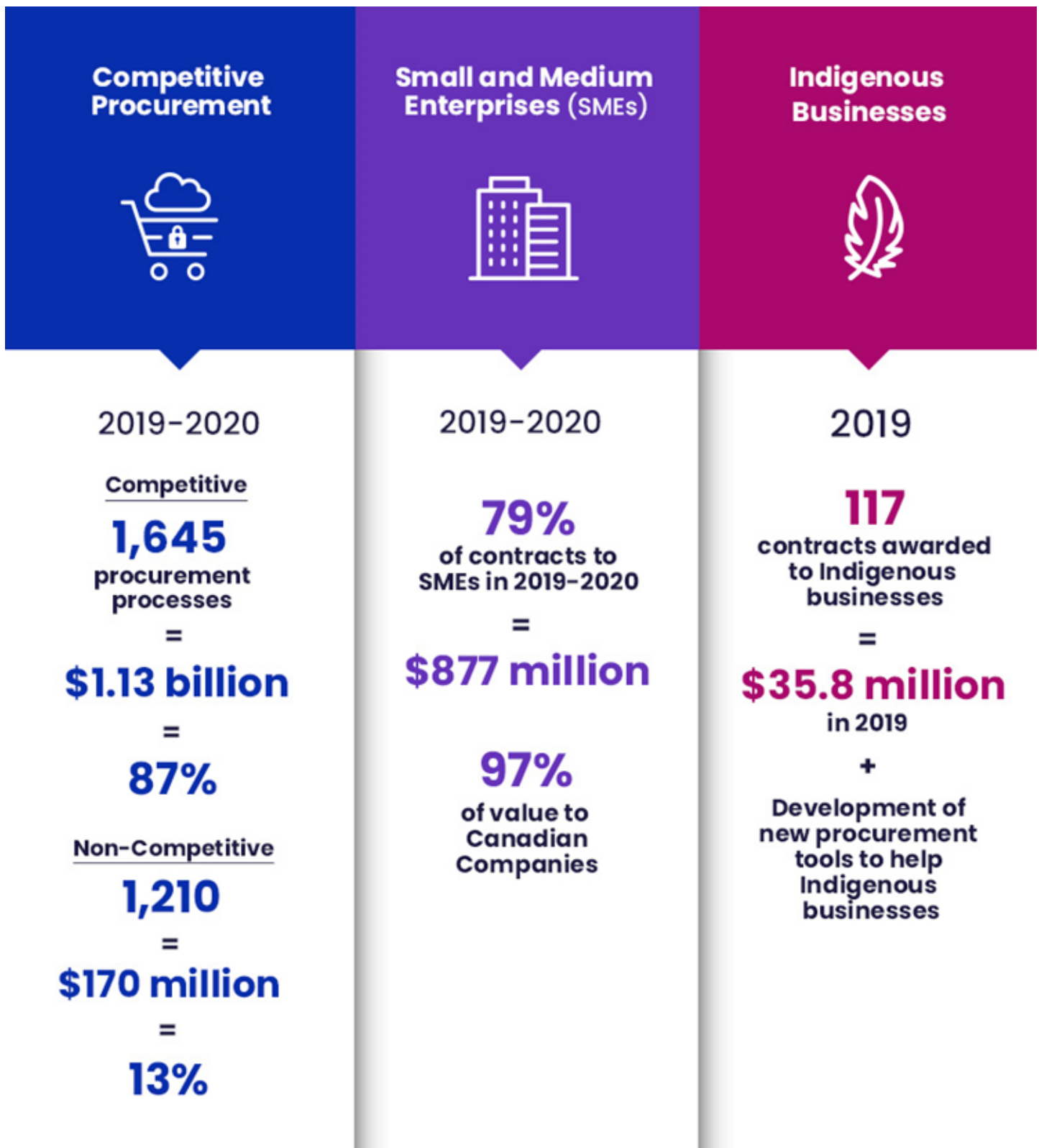
Myth: SSC should evenly disperse contracts awards among networking vendors.

Fact: SSC conducts transparent and fair procurement processes, as per the Government of Canada’s [Contracting Policy](#). Whenever possible, SSC uses competition to get the best value for Canadians.

Key to our modernization efforts is the move toward open standards, which will open up competition to a multitude of networking vendors, increasing competition and reducing the Government of Canada’s reliance on any one vendor.



SSC Procurement by the numbers



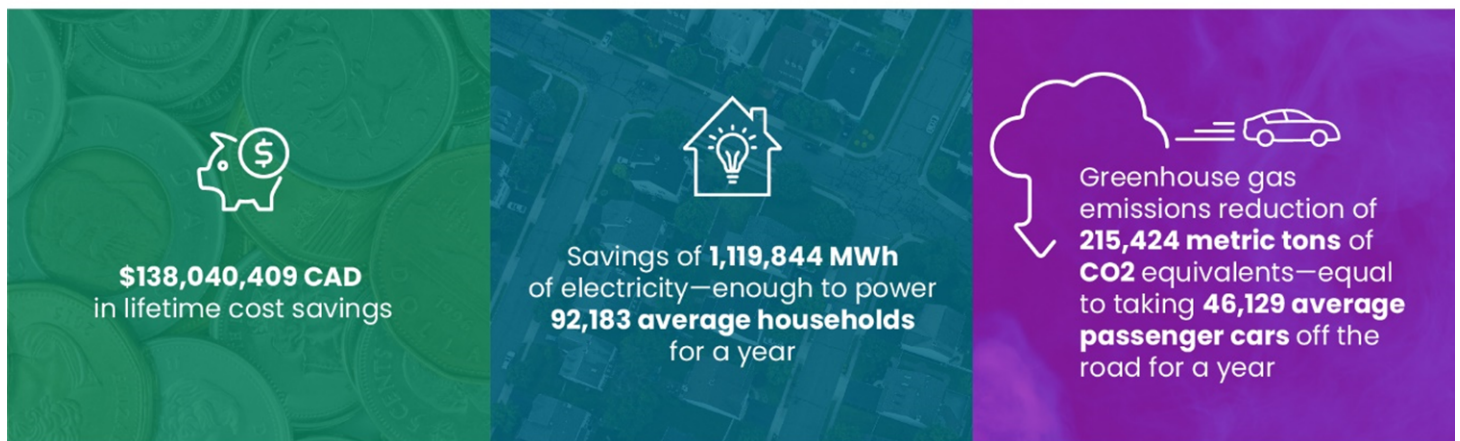
Green Procurement

SSC supports the [Greening Government Strategy](#), led by the Treasury Board of Canada Secretariat.

By purchasing IT products that meet sustainability certifications (Green Electronics Council) SSC is using its buying power to help reduce the environmental impacts of Government of Canada IT infrastructure. The industry-certified products purchased by SSC from 2014-2020 will consume less energy throughout their lifetime, resulting in:

Saving Energy

EPEAT's requirement that registered products meet, and often exceed, the latest ENERGY STAR specifications means these products will consume less energy throughout their lifetime, resulting in:



Environmental Impact

Over their lifetime, compared to products that do not meet EPEAT criteria, the EPEAT-registered IT products purchased by Shared Services Canada in 2014 – 2019 will result in environmental impact reductions including:

